REMARKS

I. Claim Rejections - 35 USC § 102

Requirements for Prima Facie Anticipation

A general definition of *prima facie* unpatentability is provided at 37 C.F.R. §1.56(b)(2)(ii):

> A *prima facie* case of unpatentability is established when the information *compels a conclusion* that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability. (*emphasis added*)

"Anticipation requires the disclosure in a single prior art reference of each element of the claim under consideration." *W.L. Gore & Associates v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303, 313 (Fed. Cir. 1983) (citing *Soundscriber Corp. v. United States*, 360 F.2d 954, 960, 148 USPQ 298, 301 (Ct. Cl.), *adopted*, 149 USPQ 640 (Ct. Cl. 1966)), *cert. denied*, 469 U.S. 851 (1984). Thus, to anticipate the applicants' claims, the reference cited by the Examiner must disclose each element recited therein. "There must be no difference between the claimed invention and the reference disclosure, as viewed by a person of ordinary skill in the field of the invention." *Scripps Clinic & Research Foundation v. Genentech, Inc.*, 927 F.2d 1565, 18 USPQ 2d 1001, 1010 (Fed. Cir. 1991).

To overcome the anticipation rejection, the applicants need only demonstrate that not all elements of a *prima facie* case of anticipation have been met, *i.e.*, show that the reference cited by the Examiner fails to disclose every element in each of the applicants' claims. "If the examination at the initial state does not produce a prima face case of unpatentability, then without more the applicant is entitled to grant of the patent." *In re Oetiker*, 977 F.2d 1443, 24 USPQ 2d 1443, 1444 (Fed. Cir. 1992).

Requirements for Inherency-Based Anticipation

There are a number of factors that must be considered when attempting to establish inherency as a basis for anticipation. Inherency should only be applied under very limited circumstances. That is, inherency permits in very limited circumstances, an invention to be anticipated by prior art that is lacking minor, well-known features in the claimed invention. If the "missing subject matter" is "inherent" or necessarily disclosed in the prior art reference, then anticipation can exist. As stated by the Federal Circuit (see In re Sun USPQ2d 1451, 1453 (Fed. Cir. 1983)

> ...To serve as an anticipation when the reference is silent about the asserted inherent characteristic, such gap in the reference may be filled with recourse to intrinsic evidence. Such evidence must make clear that the missing descriptive matter is necessarily present in the thing described in the reference and that it would be so recognized by persons of ordinary skill.

In this regard, the CCPA has added that "'[i]nherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient". See In re Oelrich, 666 F.2d 578, 581, 212 USPQ 323, 326 (C.C.P.A. 1981) (quoting Hansgrig v. Kemmer, 102 F.2d 212, 214, 40 USPQ 665, 667 (C.C.P.A. 1930). That is, the missing element or function must necessarily result from the prior art reference.

Additionally, when an Examiner's rejection relies on inherency, it is incumbent upon the Examiner to point to the page and line of the prior art that justifies the rejection based on an inherency theory. The Examiner must not leave the Applicant to guess at the basis of the inherency rejection.

The fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. *In re Rijckaert*, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993) (reversed rejection because inherency was based on what would result due to optimization of conditions, not what was necessarily present in the prior art); *In re Oelrich*, 666 F.2d 578, 581-82, 212 USPQ 323, 326 (CCPA 1981). "To establish

inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.' " *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999) (citations omitted).

"In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art." *Ex parte Levy,* 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (emphasis in original).

Berardi

The Examiner rejected claims 26-34 under 35 U.S.C. §102(e) as being anticipated by Berardi et al. (U.S. Patent Application No. 2003/0167207), hereinafter referred to as "Berardi".

The Examiner argued that Berardi shows a method for providing access to a financial transaction, where the system includes two versions of the transponder 102. The Examiner admitted that the first embodiment of transponder 102 does not include a fingerprint reader (citing FIG. 2); the Examiner interpreted this as a badge. The Examiner stated that the second embodiment of transponder 102 includes a fingerprint reader (citing FIG. 9); this is interpreted by the Examiner s a keyfob.

The Examiner argued that the FIG. 9 transponder sends the fob ID (citing stored in memory 214) with the fingerprint so both can be authenticated. The Examiner stated that when the data is read from the transponder, a comparison is made to authorize financial access, arguing that this meets the limitation of

determining if the received code is authentic and providing access upon authentication.

The Examiner argued that if the data is from a badge, the authorization step compares account data (or the transponder ID) (citing paragraph [0059]), and if the data is from a keyfob, the authorization step compares the fingerprint data (citing paragraph 141). It is the Examiner's position that in order to compare the received data from the FIG. 9 transponder with stored fingerprint data, a decision inherently is made that the data received includes fingerprint data. The Examiner stated that this meets the limitation of determining if the code is from a badge or keyfob.

The Applicant respectfully disagrees with this assessment and notes that claim 26 has been amended to change the transmission of the RF signal from the alternative of a first or second type of access device to the claiming of both a first type and a second type of access device. Claim 26 includes the limitation "transmitting an RF signal containing an authentication code from a first type of access device and a second type of access device". This is disclosed in the Applicant's FIG. 4.

Additionally, claim 26 include the further limitation of "wherein the first type of access device and the second type of access device utilize the same RF protocol". This is disclosed in the Applicant's specification in paragraph [0027] as follows:

> "As can be seen, the reader 12 of the security system 10 as described above is capable of performing the functions of both a badge reader and a keyfob receiver such that the reader 12 uses the same RF protocol in interacting with the badge 20 and the keyfob 24. Accordingly, the reader 12 is a dual-technology reader that is able to provide a simple low-cost badging technology and a higher security level solution that provides significantly higher authentication reliability using the same door reader hardware. Consequently, a supplier of access security systems can maintain a smaller inventory that includes badges, keyfobs, and only one type of reader. Moreover, a user can easily increase the level of security by simply substituting or adding keyfobs to its security system."

The Examiner has argued that claim 26 has previously claimed the alternative, whereas Berardi has disclosed the alternative in the different disclosed

embodiments. The Applicant submits that Berardi does not disclose the limitation of amended claim 26 as Berardi fails to disclose transmitting an RF signal containing an authentication code from a first type of access device *and* a second type of access device; i.e. the claim is not in the alternative. In order for Berardi to anticipate the Applicant's claim 26 under §102, Berardi *must* disclose this method limitation wherein an RF signal is transmitted from a first type and a second type of access device.

Berardi does not disclose that the first type and the second type of access devices utilize the same RF protocol. As Berardi teaches that these are two non-compatible embodiments, there would be no reason within the Berardi reference to utilize the same RF protocol.

Additionally, the Examiner has stated that a decision is inherently made in Berardi that the data received includes fingerprint data. That is not the limitation of claim 26. Claim 26 includes the further limitation of the method step of "determining whether the authentication code is of a first type or of a second different type". Berardi does not include the disclosure of this limitation. There is no *determination* (inherent or not) disclosed in the Berardi reference as to whether the authentication code is of a first or a second type. It is not inherent as Berardi discloses two *non-compatible* embodiments. If one system of Berardi is utilized, then a first type of authentication code is utilized; a second type in the alternate embodiment. Any method disclosed in Berardi does not determine and is incapable of making the determination of whether the authentication code is a first type or a second type. The point is not whether Berardi discloses a first type and a second type as alternative embodiments; the point is whether Berardi discloses the limitation of "determining" if there is a first type or a second type. The action of the third step of claim 26 is "determining". the method step of "determining" *must* be disclosed within the Berardi reference in order for a *prima facie* case of anticipation under 35 U.S.C. §102(e). Berardi does not disclose this limitation.

Claim 26 includes the next method step of "processing the authentication code in a first manner if the authentication code is of the first type and processing the authentication code in a second different manner if the authentication code is of the second different type". The Examiner has cited Berardi for the disclosure of different embodiments; however, with the different non-compatible embodiments of Berardi the step of processing a first type in a first manner and processing a second type in a second manner is not disclosed. At the very least, utilizing the Examiner's argument, Berardi could only disclose processing in a first manner or processing in a second manner. In order to anticipate the Applicant's claim 26, Berardi must disclose processing in both a first and a second manner. Berardi does not disclose a *step* of processing in a first manner and processing in a second manner.

Therefore, the Applicant submits that Berardi does not disclose the following method steps: 1) transmitting an RF signal containing an authentication code from a first type of access device and a second type of access device; 2) wherein the first type of access device and the second type of access device utilize the same RF protocol 3) determining whether the authentication code is of a first type or of a second different type; and 4) processing the authentication code in a first manner if the authentication code is of the first type and processing the authentication code in a second different manner if the authentication code is of the second different type.

Berardi therefore fails in the aforementioned *prima facie* anticipation test as each and every limitation of the Applicant's claim 26 is not disclosed. Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §102(e) rejection of claim 26 based on the Berardi reference be withdrawn.

Regarding claims 27-31, the Applicant notes that the argument presented above applies equally against the rejections of dependent claims 27-31. As argued above, Berardi fails to disclose each and every limitation of the Applicant's independent claim. Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §102(e) rejections of claims 27-31 based on the Berardi reference be withdrawn.

Regarding claim 32, the Applicant notes again that the argument presented above applies equally against the rejection of claim 32. The Applicant notes that claim 32 has been amended similar to claim 26 with the further limitation of "wherein the keyfob and the badge utilize the same RF protocol". As argued above, Berardi does not disclose that the badge and the keyfob utilize the same RF protocol.

Additionally, the Applicant points out to the Examiner that claim 32 includes the limitation of processing the authentication code in a first manner if the authentication code is derived from the keyfob and processing the authentication code in a second manner if the authentication code is derived from the badge. Berardi discloses processing in a first manner or processing in a second manner.

Therefore, the Applicant submits that Berardi fails in the aforementioned anticipation test as each and every limitation of the Applicant's claim 32 is not disclosed. Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §102(e) rejection of claim 32 based on the Berardi reference be withdrawn.

Regarding claim 33-34, the Applicant notes that the argument presented above applies equally as these claims are dependent upon claim 32. Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §102(e) rejections of claims 33-34 based on the Berardi reference be withdrawn.

II. Claim Rejections - 35 USC § 103

Requirements for Prima Facie Obviousness

The obligation of the examiner to go forward and produce reasoning and evidence in support of obviousness is clearly defined at M.P.E.P. §2142:

> "The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness."

The U.S. Supreme Court ruling of April 30, 2007 (*KSR Int'l v. Teleflex Inc.*) states:

"The TSM test captures a helpful insight: A patent composed of several elements is not proved obvious merely by demonstrating that each element was, independently, known in the prior art. Although common sense directs caution as to a patent application claiming as innovation the combination of two known devices according to their established functions, it can be important to identify a reason that would have prompted a person of ordinary skill in the art to combine the elements as the new invention does."

"To facilitate review, this analysis should be made explicit."

The U.S. Supreme Court ruling states that it is important to identify a *reason* that would have prompted a person to combine the elements and to make that analysis *explicit*. MPEP §2143 sets out the further basic criteria to establish a *prima facie* case of obviousness:

1. a reasonable expectation of success; and

2. the teaching or suggestion of all the claim limitations by the prior art reference (or references when combined).

It follows that in the absence of such a *prima facie* showing of obviousness by the Examiner (assuming there are no objections or other grounds for rejection) and of a *prima facie* showing by the Examiner of a *reason* to combine the references, an applicant is entitled to grant of a patent. Thus, in order to support an obviousness rejection, the Examiner is obliged to produce evidence compelling a conclusion that the basic criterion has been met.

Berardi in view of Fitzgibbon

The Examiner rejected claims 1-6 under 35 U.S.C. §103(a) as being unpatentable over Berardi in view of Fitzgibbon et al. (U.S. Patent Application No. 2003/02101331 A1, hereinafter referred to as "Fitzgibbon").

The Examiner argued that Berardi shows a method for providing access to a financial transaction, where the system includes two versions of the transponder

102. The Examiner stated that the first embodiment of transponder 102 does not include a fingerprint reader (citing FIG. 2 of Berardi); the Examiner interpreted this as a badge. The Examiner stated that the second embodiment of transponder 102 includes a fingerprint reader (citing FIG. 9 of Berardi); the Examiner interpreted this as a keyfob. The Examiner argued that the FIG. 9 transponder sends fob ID (stored in memory 214) with the fingerprint so both can be authenticated. The Examiner argued that when the data is read from the transponder, a comparison is made to authorize financial access; the Examiner argued that this meets the limitation of determining if the received code is authentic and providing access upon authentication. The Examiner stated that if the data is from a badge, the authorization step compares account data or the transponder 10 (citing paragraph [0059] of Berardi). If the data is from a keyfob, the authorization step compares fingerprint data (citing paragraph [0141] of Berardi). It is the Examiner's position that in order to compare the received data from the FIG. 9 transponder with stored fingerprint data, a decision is inherently made that the data received includes fingerprint data. The Examiner argued that this meets the limitation of determining is from a badge or a keyfob.

The Examiner argued that in an analogous art, Fitzgibbon teaches an access security system where a transmitter can send codes to a garage door for access authorization. The Examiner argued that the portable transmitter (authorization module) can additionally include a fingerprint reader to send information regarding the user's fingerprint, also for authorization. The Examiner argued that Fitzgibbon includes a processor (citing FIG. 4 of Fitzgibbon) in communication with the transmitters to process data received and make an authorization determination (citing FIG. 8 of Fitzgibbon). The Examiner argued that Fitzgibbon is cited for teaching that in this type of system, the use of rolling codes can improve the security of the system. The Examiner stated that the fingerprints and rolling codes

are separately checked against databases for authenticity (citing FIG. 8 of Fitzgibbon).

Therefore, the Examiner argued that it would have bee obvious to one of ordinary skill in the art at the time of the invention to have used the fingerprint and rolling code processing of Fitzgibbon in the fingerprint entry transponder embodiment of Berardi because adding rolling code authentication increases security in the system.

The Applicant respectfully disagrees with this assessment and notes that claim 1 has been amended to include the limitation wherein the badge and the keyfob utilize the same RF protocol. The argument presented above against the §102 rejections of claims 26-34 applies equally against the rejections of claim 1-6.

As argued above, Berardi does not disclose a system wherein the badge and the keyfob utilize the *same RF protocol* as in the Applicant's amended claim 1. Additionally, the Applicant notes that claim 1 includes the limitation of a transceiver that transmits a single stimulus signal to both a badge and a fingerprint keyfob. The Examiner has argued that Berardi discloses this limitation through the separate embodiments; however, the Applicant submits that with separate embodiments there inherently could not be a *single* stimulus signal.

Claim 1 also includes the limitation of a processor that *determines* whether the received authentication code is from the badge or the fingerprint keyfob. As argued above, Berardi does not disclose a processor which determines whether the received code is from a badge or a keyfob. The Examiner has argued that a decision is inherently made in the comparison of received data with stored fingerprint data; however, the Applicant submits that as Berardi discloses two non-compatible embodiments, Berardi is *incapable* of determining if the data is from a badge or a keyfob. Berardi discloses comparing data from a fingerprint keyfob (FIG. 9) with the fingerprint data. This is disclosed in Berardi paragraph [0141] as follows:

> "In one exemplary application of the fob 102 including the biometric security system 902, the customer may place his finger on the biometric sensor to initiate the mutual authentication process between the fob 102 and the RFID reader 104, or to provide secondary verification of the user's identity. The sensor fingerprint may be digitized and compared against a digitized fingerprint stored in a database (e.g., security database 212) included on fob 102. Such comparison step may be controlled by protocol/sequence controller 208 and may be validated by authentication circuit 210. Where such verification is made, the mutual authentication between fob 102 and RFID reader 104 may begin, and the transaction may proceed accordingly. Alternatively, the comparison may be made with a digitized fingerprint stored on a database maintained by the fob 102 transaction account provider system (not shown). The digitized fingerprint may be verified in much the same way as is described above with respect to the PIN." (emphasis added)

Since Berardi, in this embodiment, *only* discloses comparing the sensor fingerprint against the database of fingerprints, the data from a badge would not be received or compared by the system. In other words, since the system of Berardi is set up *only* to receive fingerprint data in order to compare with a database of fingerprint data, why would Berardi inherently determine if the received data is from a badge or a fingerprint keyfob? In fact, the Applicant submits that not only is there not a disclosure of a determination; there *inherently* can not be a determination whether the received data is from a badge or a fingerprint keyfob. In fact, Berardi teaches *away* from the disclosure of a determination of whether the received data is from a badge or a keyfob.

The Applicant's invention, as disclosed and claimed, makes a determination of whether the data is from a badge or a keyfob. The Applicant's FIG. 4, reference item 64, clearly discloses the step of determining if the data is from a badge or a keyfob. This method step is claimed in the Applicant's claim 1 and is not disclosed (specifically or inherently) in the Berardi reference.

Therefore, the Applicant submits that as Berardi does not disclose each and every limitation, Berardi in view of Fitzgibbon fails in the aforementioned *prima facie* anticipation test as each and every limitation is not disclosed in the

combination of Berardi and Fitzgibbon. The same argument applies equally to claim 2-6, as these claims are dependent upon claim 1. Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §103(a) rejections of claims 1-6 based on the Berardi and Fitzgibbon references be withdrawn.

The Examiner rejected claims 35-37 under 35 U.S.C. §103(a) as being unpatentable over Berardi as applied to claim 32 above, and further in view of Fitzgibbon.

The Examiner argued that in an analogous art, Fitzgibbon teaches an access security system where a transmitter can send codes to a garage door for access authorization. The Examiner argued that the portable transmitter (authorization module) can additionally include a fingerprint reader to send information regarding the user's fingerprint, also for authorization. The Examiner argued that Fitzgibbon includes a processor (citing FIG. 4 of Fitzgibbon) in communication with the transmitters to process data received and make an authorization determination (citing FIG. 8 of Fitzgibbon). The Examiner cited Fitzgibbon for teaching that in this type of system, the use of rolling codes can improve the security of the system. The Examiner argued that the fingerprints and rolling codes are separately checked against databases for authenticity (citing FIG. 8 of Fitzgibbon).

The Examiner argued that therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have used the fingerprint and rolling code processing of Fitzgibbon in the fingerprint entry transponder embodiment of Berardi because adding rolling code authentication increases security in the system.

The Applicant respectfully disagrees with this assessment and notes that the argument presented above against the §102 rejection of claim 32 over Berardi applies equally against the rejections of claims 35-37 as these claims are dependent upon claim 32. As argued above, Berardi does not disclose that the badge and the keyfob utilize the same RF protocol. Also, Berardi discloses

processing in a first manner or processing in a second manner, not in a first and a second manner. The Fitzgibbon reference does not supply these required claim limitations either.

Therefore, Berardi in view of Fitzgibbon fails in the aforementioned prima facie obviousness test as each and every limitation of the Applicant's claims are not disclosed. Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §103(a) rejections of claims 35-37 based on the Berardi and Fitzgibbon references be withdrawn.

Berardi in view of Fitzgibbon and Johnson

The Examiner rejected claims 7, 9-16, 18-21 and 23-25 under 35 U.S.C. §103(a) as being unpatentable over Berardi in view of Fitzgibbon and further in view of Johnson (U.S. Patent No. 5, 890520).

The Examiner argued that Berardi shows a method for providing access to a financial transaction, where the system includes two versions of the transponder 102. The Examiner stated that the first embodiment of transponder 102 does not include a fingerprint reader (citing FIG. 2 of Berardi); this is interpreted by the Examiner as a badge. The Examiner stated that the second embodiment of transponder 102 includes a fingerprint reader (citing FIG. 9 of Berardi); this is interpreted by the Examiner as a keyfob. The Examiner argued that the FIG. 9 transponder sends the fob ID (stored in memory 214) with the fingerprint so both can be authenticated. The Examiner argued that when the data is read from the transponder, a comparison is made to authorize financial access; the Examiner argued that this meets the limitation of determining if the received code is authentic and providing access upon authentication. The Examiner argued that if the data is from a badge, the authorization step compares account data (or the transponder ID, citing paragraph [0059] of Berardi). The Examiner argued that if the data is from a keyfob the authorization step compares fingerprint data (citing paragraph

[0141] of Berardi). It is the Examiner's position that in order to compare the received data from the FIG. 9 transponder with stored fingerprint data, a decision inherently is made that the data received includes fingerprint data. The Examiner argued that this meets the limitation of determining if the code is from a badge or keyfob.

The Examiner argued that in an analogous art, Fitzgibbon teaches an access security system where a transmitter can send codes to a garage door for access authorization. The Examiner argued that the portable transmitter (authorization module) can additionally include a fingerprint reader to send information regarding the user's fingerprint, also for authorization. The Examiner argued that Fitzgibbon includes a processor (citing FIG. 4 of Fitzgibbon) in communication with the transmitters to process data received and make an authorization determination (citing FIG. 8 of Fitzgibbon). The Examiner cited Fitzgibbon for teaching that in this type of system, the use of rolling codes can improve the security of the system. The Examiner argued that the fingerprints and rolling codes are separately checked against databases for authenticity (citing FIG. 8 of Fitzgibbon).

The Examiner argued that therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have used the fingerprint and rolling code processing of Fitzgibbon in the fingerprint entry transponder embodiment of Berardi because adding rolling code authentication increases security in the system.

The Examiner argued that in an analogous art, Johnson shows a communication authentication system that includes fobs for granting account access (citing col. 2, lines 15-20 of Johnson). The Examiner argued that this permits multiple types of transponders to be used to pay for services. The Examiner further argued that therefore, having a system that operates with the different types of transponders discussed in Fitzgibbon would have been obvious to one of ordinary skill in the art at the time of the invention as suggested by Johnson.

The Applicant respectfully disagrees with this assessment and notes that independent claims 7 and 14 have been amended similar to claim 1 with the additional limitation of wherein the badge and the keyfob utilize the same RF protocol. The argument presented above against the rejections of claims 1-6 applies equally against the rejections of claims 7, 9-16, 18-21 and 23-25.

As argued above, Berardi does not disclose the following method steps: 1) wherein the badge and the keyfob utilize the same RF protocol; and 2) determining whether the authentication code is from a badge or a keyfob. Fitzgibbon and Johnson do not disclose these limitations either.

Therefore, the Applicant submits that Berardi in view of Fitzgibbon and Johnson fails in the aforementioned *prima facie* obviousness test as each and every limitation of the Applicant's claims are not disclosed. Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §103a) rejections of claims 7, 9-16, 18-21 and 23-25 based on the Berardi, Fitzgibbon and Johnson references.

Fitzgibbon in view of Johnson

The Examiner rejected claims 38-41, 45-49 and 53 under 35 U.S.C. §103(a) as being unpatentable over Fitzgibbon in view of Johnson.

The Examiner argued that Fitzgibbon teaches an access security system where a transmitter can send codes to a garage door for access authorization. The portable transmitter (authorization module) can additionally include a fingerprint reader to send information regarding the user's fingerprint, also for authorization. Fitzgibbon includes a processor (citing FIG. 4 of Fitzgibbon) in communication with the transmitters to process data received and make an authorization determination (citing FIG. 8 of Fitzgibbon). The Examiner considered a gate lock as a door lock. The Examiner cited Fitzgibbon for teaching that in this type of system, the use of rolling codes can improve the security of the system (citing FIG. 5). The Examiner stated that Fitzgibbon incorporates by reference U.S. Patent No. 5,949,349 (issued

to Farris et al.) and states that the system disclosed can be used to open the gates as described in U.S. Patent No. 5,949,349 (hereinafter referred to as "Farris). The Examiner argued that Farris discuss a plurality of authorization modules associated with a gate to allow entry into the facility (citing abstract of Farris). The Examiner argued therefore using Fitzgibbon's authorization in a plural transmitter gate or garage door opening system is taught and shown by Fitzgibbon. The Examiner argued that paragraph [0052] of Fitzgibbon discusses learning a rolling code and storing in an associated table via an address of the table, arguing that looking up in the code table is considered a shared and indexed mathematical function as claimed.

The Examiner argued that in an analogous art, Johnson shows a communication authentication system that includes fobs for granting account access (citing col. 2, lines 15-20 of Johnson). The Examiner argued that this permits multiple types of transponders to be used to pay for services. The Examiner further argued that therefore, having a system that operates with the different types of transponders discussed in Fitzgibbon would have been obvious to one of ordinary skill in the art at the time of the invention as suggested by Johnson.

Regarding claims 38-41 and 45, the Applicant respectfully disagrees with this assessment The Applicant notes that the Examiner has cited Farris for disclosing the limitation of a plurality of authorization modules; however, Farris does not disclose a plurality of *authorization modules* as in the Applicant's claim 38. Farris discloses a plurality of *actuators* not *authorization modules*. This is disclosed in the Examiner's citation from Farris, as shown in the abstract as follows:

> "A barrier movement system which is useful in provided barrier movement in environments where a first barrier such as a community gate is commonly controlled by a plurality of different actuators (transmitters) which actuators separately control other barriers such as household garage doors. The controller of the commonly controlled gate receives and contemporaneously analyzes codes in accordance with a plurality of different code format standards and at the same time analyzes the received code to determine which format is actually being received. In an embodiment only a fixed code portion of a rolling code sequence is used for actuation at the commonly controlled barrier." (emphasis added)

A module is a *program or software routine* performed on a processor. The plurality of modules in the Applicant's invention is disclosed in FIG. 4 as blocks 66 and 74. An actuator is not a module, therefore, Farris does not disclose the limitation of a plurality if authorization modules. Therefore, as Farris (incorporated by reference in Fitzgibbon) does not disclose the limitation it follows that Fitzgibbon in view of Johnson also does not disclose the limitation.

Therefore, Fitzgibbon in view of Johnson fails in the aforementioned *prima facie* obviousness test as each and every limitation of the Applicant's claim 38 is not disclosed. As claims 39-41 and 45 are dependent upon claim 38, Fitzgibbon in view of Johnson does not disclose each and every limitation of claims 39-41 and 45. Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §103(a) rejections of claims 38-41 and 45 based on the Fitzgibbon and Johnson references be withdrawn.

Regarding claims 46-49 and 53, the Applicant notes that the argument presented above applies equally against the rejections of claims 46-49 and 53 as Fitzgibbon in view of Johnson does not disclose a plurality of authorization modules as in the Applicant's independent claim 46. Additionally, the Applicant notes that claim 46 has been amended to include the limitation of "providing at least two types of authorization devices wherein said at least two types of authorization devices transmit data to said access device utilizing the same RF protocol".

The Applicant submits that neither Fitzgibbon nor Johnson disclose: 1) at least two types of authorization devices and 2) wherein the devices utilize the same RF protocol. Therefore, Fitzgibbon in view of Johnson fails in the aforementioned prima facie obviousness test as each and every limitation of the Applicant's claims 46-49 and 53. Based on the foregoing, the Applicant respectfully requests that the

35 U.S.C. §103(a) rejections of claims 46-49 and 53 based on the Fitzgibbon and Johnson references be withdrawn.

Fitzgibbon in view of Johnson/Berardi

The Examiner rejected claims 42-44 and 50-52 under 35 U.S.C. §103(a) as being unpatentable over Fitzgibbon in view of Johnson as applied to claims 38 and 46 above, and further in view of Berardi.

The Examiner argued that Berardi shows an access control system including a transponder, which may be embodied in a fob, tag or card (citing paragraph [0021] of Berardi). The Examiner argued that the FIG. 9 transponder sends the fob ID (stored in memory 214) with the fingerprint so both can be authenticated, thereby suggesting a fingerprint fob.

The Examiner argued that therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have formed the Fitzgibbon controller into a key fob or a card since Berardi suggests these embodiments for an access device and such physical embodiments are recognized in the art as easily portable.

Regarding claims 42-44, the Applicant respectfully disagrees with this assessment and notes that the argument presented above against the rejections of claims 38-41 applies equally against the rejections of claims 42-44. As argued above, Fitzgibbon in view of Johnson does not disclose the limitation of a plurality if authorization modules. The Applicant submits that Berardi does not disclose the plurality of authorization modules either.

Therefore, Fitzgibbon in view of Johnson and further in view of Berardi fails in the aforementioned *prima facie* obviousness test as each and every limitation of the Applicant's claims 42-44 is not disclosed. Based on the foregoing, the Applicant

respectfully requests that the 35 U.S.C. §103(a) rejections of claims 42-44 based on the Fitzgibbon, Johnson and Berardi references be withdrawn.

Regarding claims 50-52, the Applicant notes that the argument presented above against the rejections of claims 46-49 and 53 applies equally against the rejections of claims 50-52. As argued above, neither Fitzgibbon nor Johnson disclose: 1) at least two types of authorization devices and 2) wherein the devices utilize the same RF protocol. Berardi does not disclose the limitations and therefore Fitzgibbon in view of Johnson and further in view of Berardi does not disclose theses limitations.

Therefore, Fitzgibbon in view of Johnson and further in view of Berardi fails in the aforementioned *prima facie* obviousness test as each and every limitation of the Applicant's claims 50-52. Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §103(a) rejections of claims 50-52 based on the Fitzgibbon, Johnson and Berardi references be withdrawn.

III. Conclusion

In view of the foregoing discussion, the Applicant has responded to each and every rejection of the Official Action. The Applicant has clarified the structural distinctions of the present invention. Applicant respectfully requests the withdrawal of the rejections under 35 U.S.C. §102 and 35 U.S.C. §103 based on the preceding remarks. Reconsideration and allowance of Applicant's application is also respectfully solicited. A Request for Continued Examination (RCE) under 37 CFR 1.114 is also submitted herewith, including the RCE fee of $810.

Should there be any outstanding matters that need to be resolved, the Examiner is respectfully requested to contact the undersigned representative to

conduct an interview in an effort to expedite prosecution in connection with the present application.

Respectfully submitted,

Dated: November 21, 2007

Kermit Lopez
Attorney for Applicants
Registration No. 41,953
ORTIZ & LOPEZ, PLLC
P.O. Box 4484
Albuquerque, NM 87196-4484